

OFFICE OF AUDITS & ADVISORY SERVICES



COMPUTER OPERATIONS - BACKUP AND RESTORATION

FINAL AUDIT REPORT

Chief of Audits: Julie Nieminski, CPA, CIA, CFE, CISA, MPA
Senior Audit Manager: Tom Philipp, CIA, CCSA, MBA
Senior Audit Manager: Lynne Prizzia, CISA, CRISC
Senior Auditor: Franco Lopez, CPA, CIA, CISA, MBA

Intentionally Left Blank



County of San Diego

DONALD F. STEUER
CHIEF FINANCIAL OFFICER
(619) 531-5413
FAX (619) 531-5219

AUDITOR AND CONTROLLER
1600 PACIFIC HIGHWAY STE 166, SAN DIEGO, CALIFORNIA 92101-2478

TRACY M. SANDOVAL
ASST. CHIEF FINANCIAL OFFICER/
AUDITOR & CONTROLLER
(619) 531-5413
FAX (619) 531-5219

December 6, 2012

TO: Mikel D. Haas, Chief Information Officer
County Technology Office

FROM: Julie B. Nieminski
Chief of Audits

FINAL REPORT: COMPUTER OPERATIONS – BACKUP AND RESTORATION

Enclosed is our report on the Computer Operations – Backup and Restoration. We have reviewed your responses to our recommendations and have attached them to the audit report.

The actions taken and/or planned, in general, are responsive to the recommendations in the report. As required under Board Policy B-44, we respectfully request that you provide quarterly status reports on the implementation progress of the recommendations. The Office of Audits & Advisory Services will contact you or your designee near the end of each quarter to request your response.

Also attached is an example of the quarterly report that is required until all actions have been implemented. To obtain an electronic copy of this template, please contact Franco Lopez at (858) 505-6436.

If you have any questions, please contact me at (858) 495-5661.

JULIE B. NIEMINSKI
Chief of Audits

AUD:FDL:aps

Enclosure

c: Tracy M. Sandoval, General Manager/Auditor and Controller
Brian M. Hagerty, Group Finance Director, Finance & General Government

INTRODUCTION

Audit Objective The Office of Audits & Advisory Services (OAAS) completed an audit of Computer Operations – Backup and Restoration. The objective of the audit was to review the adequacy of the controls over the County's backup and restoration processes for information technology (IT) systems and data.

Background The County of San Diego's Information Technology and Telecommunication Service Agreement (Agreement) assigns responsibility for the County's IT backup and restoration processes to Hewlett Packard's Enterprise Services (HP). HP administers over 600 County backup jobs daily and manages respective offsite backup media. HP and its subcontractor AT&T maintain the County's IT systems, data, and network infrastructure in three primary data centers located in San Diego, CA; Plano, TX; and Tulsa, OK. HP is responsible for backup and restoration of the County's Mainframe, UNIX, Wintel, and AS400 systems, while AT&T manages the backup and restoration processes for the County's network.

The County's primary method for requesting data restorations is through a Help Desk ticket; typically submitted by County employees to restore individual files. HP and AT&T also conduct data restorations as needed in response to operational events at the data centers that require backup restores. These restorations are generally more comprehensive and may involve restoring application, database and/or network servers.

Audit Scope & Limitations The scope of the audit focused on backup and restoration activity for FY 2011-12. The audit was limited to testing controls over the County's backup and restoration processes managed by HP and AT&T. The audit did not review backup and restoration processes that occur outside of the Agreement.

The audit was conducted in conformance with the International Standards for the Professional Practice of Internal Auditing prescribed by the Institute of Internal Auditors as required by California Government Code, Section 1236. OAAS also based their assessment on recommended IT controls from the IT Governance Institute's Control Objectives for Information and related Technology 4.1 (COBIT) and the National Institute of Standards and Technology's (NIST) Guide for Assessing the Security Controls in Federal Information Systems and Organizations.

Methodology OAAS performed the audit using the following methods:

- Reviewed the Agreement as well as relevant business process documents from HP and AT&T.
- Interviewed County, HP, and AT&T stakeholders.

- Assessed the risks in the HP and AT&T backup and restoration processes.
- Performed detailed analysis of HP and AT&T backup and restoration information, such as backup job logs.
- Identified, reviewed, and tested controls over the County's backup and restoration processes for information technology systems and data, such as media handling, reporting, and restoration testing.

AUDIT RESULTS

Summary

Within the scope of the audit, controls over the HP and AT&T backup and restoration processes for the County's IT systems and data need strengthening. Specific issues were identified in the areas of: reporting and correcting backup job failures, application restoration testing for midrange servers, and AT&T backup and restoration security.

To strengthen current controls and improve the effectiveness of HP and AT&T backup and restoration processes, OAAS has the following findings and recommendations.

Finding I:

Backup Failures are Not Reported or Recorded in Accordance with the Agreement

A review of backup job completion logs from August 2011 identified inconsistencies in MASL 30 (Back-up Completion) reporting and the prompt correction of backup failures. These inconsistencies included:

- **MASL 30 Reported Results are Not Sufficiently Supported**

In August 2011, MASL 30 reported 14,537 out of 14,742 backup jobs scheduled completed successfully on 420 servers. This resulted in a reported success rate of 99%. However, a review of August 2011 backup job completion logs for these servers identified 756 actual backup job failures, versus the 205 failures reflected in the MASL report. Based upon our review of the available backup job completion logs for these servers, it appears that the success rate was 95% and not 99% as reported.

In their response to the audit testing results, HP maintained that MASL 30 was accurately reported for August 2011 and that HP further processes backup completion logs in a working file to calculate monthly MASL 30 reports. When OAAS requested working files supporting HP's MASL 30 calculation for August 2011, HP indicated files are only retained for 60 days and were no longer available, which is not in compliance with the Recordkeeping and Audit Rights section of the Agreement.¹

¹ Agreement Part IV, Section 13.1

- **MASL 30 Reported Results are Incomplete**

August 2011 backup job completion logs also included an additional 246 servers which were excluded in MASL 30 results. The logs indicated that these servers had 519 actual backup job failures out of 11,137 backup jobs scheduled, for a success rate of 95%. The review also noted that the County's Mainframe, AS400, and VAX platform's backup completion performance are excluded in MASL 30 results.

- **Required Help Desk Tickets are Not Created for Backup Failures**

From a sample of 30 servers with backup jobs that failed to complete on two or more consecutive days, Help Desk tickets were not created for 31 of 64 (48%) sets of backup failures.

The Agreement requires a backup success rate of 99% and that all servers and platforms being backed up are included in MASL 30 reporting.² The Agreement also requires HP to retain and maintain accurate records and documents relating to performance of services for at least six years after final payment.³ Additionally, HP policy requires that a Help Desk ticket be created when a backup fails for two or more consecutive days.

The County relies on the accuracy, completeness, and supportability of MASL reporting to ensure backups are conducted in accordance with the Agreement. This helps to ensure that backup data can be restored as needed. The inability to identify and correct backup failures in a timely manner could result in loss of data or productivity. Reporting inaccurate success rates can result in HP not taking corrective action.

Recommendation:

The County Technology Office (CTO) should ensure adequate controls are in place to achieve backup completion success rates specified in the Agreement. To accomplish this, the CTO should implement the following:

1. Ensure HP retains and maintains accurate records and documents relating to performance of services to allow for verification of reported MASL results, in accordance with the Agreement.
2. Ensure backup related MASLs are completely reporting on all server platforms as required by the Agreement. This includes verifying that the backup completion performance for the Mainframe, AS400, and VAX platforms are incorporated into MASL 30 results.
3. Ensure that HP is conducting timely monitoring of backup jobs and addressing backup failures, as appropriate. This includes verifying that HP creates a Help Desk ticket when a backup job fails for two or more consecutive days, as required by HP policy.

² Agreement Schedule 4.3, Exhibit 4.3.8, Section 1.3.5.22

³ Agreement Part IV, Section 13.1(b)

Finding II:**Application Recovery Testing and Reporting Needs Improvement**

Offsite backup tape restoration testing is not regularly conducted, and recent application recovery testing results did not provide evidence that contracted requirements could be met.

To assess HP's ability to achieve their contracted objectives,⁴ OAAS reviewed the results of HP midrange recovery testing conducted in December 2011 for two County applications. Review of midrange testing results identified the following:

- The Recovery Point objective for one of two County applications was not met because a backup tape was not available for the date selected. A tape from a subsequent date was selected in order to continue testing.
- The Recovery Time objectives for the two applications were reported as met; however, supporting documentation did not provide sufficient detail or clear evidence that the applications were recovered within the required timeframe.
- HP recovery testing results did not include evidence that the restored applications were ready for production (e.g., processing of transactions by County users).

NIST specifies that organizations should conduct information system backup testing, with a defined frequency, to verify backup media reliability and information integrity. However, the County does not require periodic testing under the current Agreement.

Recommendation:

The CTO should work with HP to create a periodic backup and restoration testing process that verifies backup media existence, reliability, and information integrity. This should include, but is not limited to:

1. Conducting backup testing in accordance with a County-defined frequency.
2. Reporting in sufficient detail on backup and restoration testing results.
3. Verifying the production usability of recovered applications and backup data.
4. Assessing the reasonableness of the process and amending the Agreement as needed.

⁴ Primary objectives include recovery point objectives (RPO) and recovery time objectives (RTO). RPO is the maximum tolerable period in which data might be lost due to an incident. RTO is the duration of time within which a system must be restored after an incident in order to avoid consequences associated with a break in business continuity.

Finding III:**AT&T Backup Tapes Transport Security Needs Improvement**

Network backup tapes are transported from the AT&T Point of Presence (POP) data center to an offsite tape storage location and retained in a fireproof safe. However, it was observed that the container used during transport was an unsecured cardboard box that provided minimal protection of the data during transit.

AT&T previously utilized a vendor to provide secured data transport, but recently modified their process by eliminating the transport vendor and assuming full transport responsibility. The Agreement requires secure transportation of backups.⁵ Additionally, COBIT recommends that organizations define and implement policies and procedures to identify and apply security requirements applicable to the receipt, processing, storage and output of data. Inadequate security of backup data could result in damaged, lost, misused, or misappropriated data.

Recommendation:

The CTO should work with HP to implement adequate security policies and procedures to ensure the backup tape transportation process is secure. HP's subcontractors should be held accountable for complying with HP policies and procedures.

Office of Audits & Advisory Services

Compliance **R**eliability **E**ffectiveness **A**ccountability **T**ransparency **E**fficiency

VALUE

⁵ Agreement Schedule 4.3, Section 6.8.2.10

DEPARTMENT'S RESPONSE



County of San Diego

County Technology Office
MIKEL HAAS
Chief Information Officer
619-581-5570 office

1600 PACIFIC HIGHWAY, ROOM 306F, SAN DIEGO, CA 92101-2472

Office of the CIO
Business Advisory Services
Communications
Enterprise Architecture & Technology
Financial & Contract Mgmt Services
Risk Management
Service Management

RECEIVED

DEC 06 2012

OFFICE OF AUDITS &
ADVISORY SERVICES

11/27/2012
Ref: 12-IA-313

To: Julie B. Nieminski
Chief of Audits
County of San Diego

From: Mikel Haas
Chief Information Officer
County Technology Office

Subject: County Technology Office Response to Audit Recommendations: Computer Operations – Backup and Restoration.

Dear Ms. Nieminski,

In accordance with the Board of Supervisor Policy B-44 the following are the County Technology Office's written response addressing the audit findings and recommendations contained in Draft Audit Report # A11-014 (Computer Operations – Backup and Restoration)

Finding I: Backup Failures are Not Reported or Recorded in Accordance with the Agreement

OAAS Recommendation:

The County Technology Office (CTO) should ensure adequate controls are in place to achieve backup completion success rates specified in the Agreement. To accomplish this, the CTO should implement the following:

1. Ensure HP retains and maintains accurate records and documents relating to performance of services to allow for verification of reported MASL results, in accordance with the Agreement.
2. Ensure backup related MASLs are completely reporting on all server platforms as required by the Agreement. This includes verifying that the backup completion performance for the Mainframe, AS400, and VAX platforms are incorporated into MASL 30 results.
3. Ensure that HP is conducting timely monitoring of backup jobs and addressing backup failures, as appropriate. This includes verifying that HP creates a Help Desk ticket when a backup job fails for two or more consecutive days, as required by HP policy.

Action Plan: The County Technology Office agrees with the audit findings for this item and will implement the recommendations as outlined in the OAAS Recommendations.

Planned Completion Date: 01/18/13

Finding II: Application Recovery Testing and Reporting Needs Improvement

OAAS Recommendation:

The CTO should work with HP to create a periodic backup and restoration testing process that verifies backup media existence, reliability, and information integrity. This should include, but is not limited to:

1. Conducting backup testing in accordance with a County-defined frequency.
2. Reporting in sufficient detail on backup and restoration testing results.
3. Verifying the production usability of recovered applications and backup data.
4. Assessing the reasonableness of the process and amending the Agreement as needed.

Action Plan: The County Technology Office agrees with the audit findings for this item and will implement a periodic process to verify backup media existence, reliability and information integrity.

Planned Completion Date: 3/31/13

Finding III: AT&T Backup Tapes Transport Security Needs Improvement

OAAS Recommendation:

The CTO should work with HP to implement adequate security policies and procedures to ensure the backup tape transportation process is secure. HP's subcontractors should be held accountable for complying with HP policies and procedures.


Action Plan: The County Technology Office agrees with the audit findings for this item and will require HP has its partner AT&T put in place a process that will comply with the appropriate security policies in transporting backup tapes.

Planned Completion Date: 12/30/12

Contact Information for Implementation: Richard Corsi, Finance & Contract Manager

If you have any questions please contact Richard Corsi at (619) 595-4628

Regards,


Mikel Haas,
Chief Information Officer